

SEALED

United States District Court

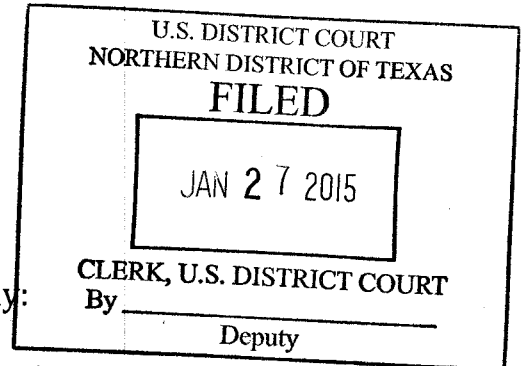
NORTHERN DISTRICT OF TEXAS

In the Matter of the Search of

A HEWLETT PACKARD PAVILION DV7-6C95DX
LAPTOP COMPUTER WITH SERIAL NUMBER
2CE21616QT, AN HTC CELLULAR TELEPHONE WITH
SERIAL NUMBER HT2BMW600489, AND AN ATIVA
4GB THUMBDRIVE CONTAINING THE
ALPHANUMERIC SEQUENCES AJDON4GB-000-1002P
AND 33249-4GBCA-0211,
CURRENTLY LOCATED AT THE FEDERAL BUREAU
OF INVESTIGATION, ONE JUSTICE WAY, DALLAS,
TEXAS, 75220

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

CASE NUMBER: 3-15-MJ-042-BN



I, JASON IBRAHIM being duly sworn depose and say:

I am a Special Agent with the Federal Bureau of Investigation
and have reason to believe that on the property or premises described as follows:

- a Hewlett Packard Pavilion DV7-6C95DX laptop computer with serial number 2CE21616QT,
- an HTC cellular telephone with serial number HT2BMW600489, and
- an ATIVA 4GB thumb drive containing the alphanumeric sequences AJDON4GB-000-1002P and 33249-4GBCA-0211.

in the NORTHERN DISTRICT OF TEXAS there is now concealed a certain property, namely those more specifically described in the attached *Attachment A* which are the evidence, fruits, and instrumentalities of crimes concerning violations of 18 U.S.C. § 875(d) and 18 U.S.C. § 1951(a).

The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT

Jason Ibrahim
Signature of Affiant - JASON IBRAHIM
Special Agent,
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence

January 27, 2015
Date and Time Issued

at Dallas, Texas
City and State

DAVID L. HORAN, U.S. Magistrate Judge
Name and Title of Judicial Officer

[Signature]
Signature of Judicial Officer

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

IN THE MATTER OF THE SEARCH OF
A HEWLETT PACKARD PAVILION DV7-6C95DX
LAPTOP COMPUTER WITH SERIAL NUMBER
2CE21616QT, AN HTC CELLULAR TELEPHONE WITH
SERIAL NUMBER HT2BMW600489, AND AN ATIVA
4GB THUMBDRIVE CONTAINING THE
ALPHANUMERIC SEQUENCES AJDON4GB-000-1002P
AND 33249-4GBCA-0211,
CURRENTLY LOCATED AT THE FEDERAL BUREAU
OF INVESTIGATION, ONE JUSTICE WAY, DALLAS,
TEXAS, 75220

NO.

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Jason Ibrahim, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the following three electronic devices (Target Devices) which are currently in law enforcement possession, and the extraction from that property of electronically-stored information described in Attachment A:

- a Hewlett Packard Pavilion DV7-6C95DX laptop computer with serial number 2CE21616QT,
- an HTC cellular telephone with serial number HT2BMW600489, and
- an ATIVA 4GB thumb drive containing the alphanumeric sequences AJDON4GB-000-1002P and 33249-4GBCA-0211.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), duly appointed and acting according to law. I have been a Special Agent for over eleven years, and am currently assigned to the Dallas Division of the FBI and more specifically to the FBI's Dallas Violent Crimes Task Force (DVCTF), where I investigate federal offenses such as bank robbery, kidnapping, and extortion, including cyber-extortion cases.

3. The applied-for warrant would authorize the forensic examination of the Target Devices for the purpose of identifying electronically-stored data particularly described in Attachment A. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. My duties as a Special Agent with the FBI include the investigation of LYNN STANLEY FAUST (FAUST) in the case of *United States v. William Laurence Stanley and Lynn Stanley Faust*, Case Number 3:14-CR-113-N (02). As the case agent in the investigation, I am familiar with the facts of the investigation involving the criminal activities of FAUST.

CHARGES

5. On or about March 26, 2014, a federal Grand Jury in the Northern District

of Texas found probable cause to charge FAUST in an Indictment,¹ with one count of Aiding and Abetting and Transmitting Threats in Interstate and Foreign Commerce, in violation of 18 U.S.C. §§ 875(d) and 2, and one count of Aiding and Abetting and Hobbs Act – Extortion, in violation of 18 U.S.C. §§ 1951(a) and 2.

INVESTIGATION

6. During the course of this investigation, I have interviewed numerous persons, including multiple witnesses in the charged offenses. I have also reviewed the reports of additional witness interviews conducted by other FBI agents working on this investigation. In addition, I have reviewed the results of Court-authorized search warrants for numerous e-mail accounts used by FAUST and her brother William Laurence Stanley (Stanley), such as reputationrewards@gmail.com, reputationlynn@gmail.com, reputationmatrix@gmail.com, completereputation@gmail.com, postingshowspace@gmail.com, and lynn.faust@yahoo.com. I have reviewed e-mails provided to me by the victim-business, Generational Equity, as well as listened to recordings of consensually-monitored telephone conversations between Generational Equity and Stanley and Generational Equity and FAUST. All of the items reviewed by me corroborate the information provided by the individuals interviewed.

7. The evidence obtained in the investigation revealed that between on or

¹ Said Indictment was filed in United States District Court for the Northern District of Texas, Dallas Division.

about December 13, 2013, and continuing through on or about February 28, 2014, FAUST and her brother Stanley made repeated threats to harm Generational Equity by damaging its online reputation and thereby creating economic harm.

OFFENSE CONDUCT BACKGROUND

8. As background information, Generational Equity originally dealt with Stanley on or about November 4, 2009, when it entered into a contractual arrangement with Stanley for his search engine optimization (SEO) services and online-reputation management. Generational Equity hired Stanley to improve its online reputation through search results. In 2010, Generational Equity determined that Stanley had acted outside the scope of his contracted duties, and Generational Equity terminated the contract. However, Stanley would not accept the termination and demanded additional payments from Generational Equity to leave without any incident. Stanley stated that he would do more harm to the company if he did not receive the payments. Generational Equity knew that Stanley had the ability to damage their reputation by publishing negative Internet posts about the company. Therefore, in or about November 2010 and continuing until in or about January 2011, Generational Equity made four payments to Stanley totaling \$80,000 in order for Stanley to “go away.” Affiant reviewed many e-mails and financial documents provided by Generational Equity supporting Stanley’s past relationship with Generational Equity.

FACTS SUPPORTING CURRENT CHARGES

9. Three years later, on December 13, 2013, Generational Equity received an

e-mail from an individual identifying himself as “William Davis” and using e-mail address reputationrewards@gmail.com, stating that Generational Equity owed him \$28,000 because it had hired four individuals from a separate company, The March Group, that purportedly owed him \$28,000. The e-mail also threatened that Generational Equity’s failure to pay would result in its business being placed on fifty (50) complaint websites. This threat essentially stated that the extorter would utilize search engine optimization (SEO) techniques to harm Generational Equity’s reputation.

10. On December 14, 2013, Generational Equity received another e-mail from reputationrewards@gmail.com, this time identifying the sender as “William Laurence,” stating that he had been “chasing these guys for years to get the money they owe me for my reputation work.... I have done business with your company in the past so I am well aware of how things work.... I am a reputation expert and probably the best in the business. I assure you it is in your best interest to make sure I am not unhappy.” The threatening message was signed “Bill.”

11. On December 17, 2013, an employee from Generational Equity received two responses from “Bill” via the reputationrewards@gmail.com account, one confirming that he was Bill Stanley (despite the sender name still saying “William Laurence”), and the other stating “now that I have found them I do not care how I get paid... but I am not going without getting paid.... They have avoided payment and stayed in hiding long enough.” Based on the message received on December 14, 2013, and the extorter’s confirmation that he was Bill Stanley (i.e., the individual that

Generational Equity had previously paid to “go away” in late 2010 to early 2011), the company feared that the extorter was in fact, Stanley, and therefore capable of following through on his threats.²

12. On January 3, 2014, Stanley, using the e-mail account reputationrewards@gmail.com, sent another e-mail to Generational Equity threatening to “start posting Monday at 5:00 p.m. if I do not hear from you or receive payment of the invoice below.” Based on the date received, the deadline date was interpreted by Generational Equity as Monday, January 6, 2014. Generational Equity responded by e-mail to Stanley at reputationrewards@gmail.com on Monday, January 6, 2014, in an attempt to delay the threatened conduct. In its e-mail response to Stanley, Generational Equity claimed it had just received and read Stanley’s e-mail and needed more time to review the issues. Generational Equity requested supporting documentation for the alleged debt of \$28,000. Stanley responded from the reputationrewards@gmail.com account stating that the debt “must be paid” and provided a contact phone number of 361-444-3559. Generational Equity then called the number provided by Stanley and left a voice mail message for him.³

² The extorter is referred to as Stanley throughout the remainder of the affidavit for the reasons discussed both above and below, which include (1) the sender’s identification of himself as Stanley in an e-mail to Generational Equity, (2) the receipt of money in Romania in the name of “William L. Stanley” via MoneyGram, which requires a recipient to show proof of identification, and (3) Stanley’s postarrest admission that he had sent threatening e-mails to Generational Equity and that he had received money from Generational Equity in Romania via MoneyGram.

³ Checks on telephone number 361-444-3559 indicated that it was a Voice over Internet Protocol (VoIP) number operated on the network of Bandwidth.com. Checks with Bandwidth.com’s Legal Department

13. On January 12, 2014, Stanley sent an e-mail to Generational Equity through the reputationrewards@gmail.com account and acknowledged the voice mail messages from Generational Equity, but stated he did not want to “spend a lot of time playing phone tag.” In the e-mail message signed by “Bill,” Stanley continued, “I do not want this to turn into a pissing contest over this money and I really do not want to start posting a bunch of stuff that you are going to just ask me to take down later (which I will not be able to do once posted). So just pay me the money and call it a day. Take it from the March Group and just suck it up. The one thing I do know is if I have to spend a lot of time on this the number is going to increase. Do your company a favor and just pay it while it is cheap and easy. Your company is robbing people blind and to pay me what is owed is in your best interest. Just consider it cost of doing business.”

14. On January 14, 2014, an individual identifying herself as “Lynn Michaels” (who has since been identified as Stanley’s sister, LYNN STANLEY FAUST) e-mailed Generational Equity from e-mail address reputationrewards@gmail.com, asking Generational Equity to contact her at reputationlynn@gmail.com to schedule a telephone call.⁴

revealed that, by virtue of a paid contractual agreement, the number had been assigned to one of its wholesale customers, Google, Inc./GoogleVoice.

⁴ Affiant has reviewed multiple e-mails obtained from a Court-authorized search warrant on the e-mail account reputationlynn@gmail.com, wherein the user of that e-mail account identifies herself as LYNN FAUST. For instance, on July 31, 2013, an e-mail was sent from reputationlynn@gmail.com to [REDACTED]@conocophillips.com stating, “My name is Lynn Faust. I work with Bill Stanley. I am sending the change of address and direct deposit order to you under separate cover. Could you please tell me the current balance of Mr. Stanley's account as of today.” In addition, as discussed in more detail

15. A Generational Equity employee e-mailed FAUST back at reputationlynn@gmail.com to schedule a telephone call and subsequently engaged in several telephone calls with FAUST, all of which were consensually recorded. For instance, on or about January 16, 2014, FAUST called the Generational Equity employee from telephone number [REDACTED]-2380. During the call, FAUST informed the employee that Generational Equity did not have much time before Stanley did “whatever it is that he does.” When the employee asked if Stanley would follow through with the negative postings on the Internet, FAUST confirmed that Stanley had the intention to do so, saying that was indeed “what he sa[id]” he would do.

16. On or about January 22, 2014, Stanley, using the e-mail address postingshowspace@gmail.com with an associated name of “William Harris,” sent Generational Equity an e-mail stating: “Ok here is the Deal. I am going to start posting now. I guess you dont [sic] take this serious enough but I have been chasing this payment for years and am not in the mood to play games. What I should and will do if it is not paid this week is add my collection fee to the invoice which will be at least 5k. I have put a lot of time and effort into this account and I am tired of this shit. Here is the first of many posts. I will start the SEO on this post and as you can see this one on the march group it will not take long to be page 1 in google.” Below the above statements were the following two links: [https://www.\[REDACTED\]the+march+group](https://www.[REDACTED]the+march+group) and

below, Stanley admitted in a postarrest statement that his sister “LYNN FAUST” had done most of the negotiating with Generational Equity in this matter and had used the alias “Lynn Michaels” while doing so.

[http://generational-equity-\[REDACTED\]/scam-generational-equity-dallas.html](http://generational-equity-[REDACTED]/scam-generational-equity-dallas.html). The second link, which Affiant viewed on the Internet, was to a blog that identified Generational Equity as a “scam.”⁵

17. On January 23, 2014, FAUST, using the e-mail address reputationlynn@gmail.com, sent an e-mail to Generational Equity stating that Stanley was insistent that Generational Equity also submit a signed “release” to Stanley. Later that same day, FAUST, using the e-mail address reputationlynn@gmail.com, sent an e-mail to Generational Equity which contained an attachment of a Microsoft Word document entitled “GE Settlement Agreement.doc.” The attached document listed Stanley as the “Creditor” and Generational Equity as the “Debtor” and stated that the agreement “constitute[d] a compromise, settlement, and release of disputed claims.” FAUST and Generational Equity would go back and forth via e-mail on several occasions about the language in the settlement agreement/release, and at times would attach revised versions of the document, before it was ultimately signed by Generational Equity and Stanley.

18. On January 24, 2014, FAUST called Generational Equity from telephone number 306-936-2380. During the call, which was consensually recorded, a Generational Equity employee asked if any “negative postings” created by Stanley on the Internet would be removed once payment was made. FAUST replied that “if indeed something

⁵ Generational Equity officers informed Affiant that negative online postings about the company, like the ones mentioned by Stanley, could cost the company approximately \$100,000-\$200,000 per week in revenue.

was done . . . [it] can be undone.” When the employee asked if half of the payment could be made up front and the other half made after any negative postings were removed from the Internet, FAUST replied “that’s not an option” because they had allowed others to make payment that way in the past and “it just doesn’t work, once they pay the first one, then we never see the rest of the money.” FAUST also mentioned during the call that her role was to “facilitate agreements” and that she was “only getting paid on a . . . flat fee for legal services on this.”

19. That same day, FAUST again called Generational Equity, this time from an unknown telephone number. During the call, which was consensually recorded, FAUST and the same Generational Equity employee discussed methods of payment. When the employee asked if Stanley would accept a cashier’s check to avoid an overseas company wire transaction, FAUST replied that “you’d have to send it . . . FedEx to Romania, which is where [Stanley] is” and that she would have to ask Stanley if a cashier’s check would be acceptable. When the employee asked if the payment amount was \$28,000, FAUST replied that it was \$29,000 with her “fee.”

20. Later that same day, FAUST again called Generational Equity from an unknown telephone number. During the call, which was consensually recorded, FAUST told the same Generational Equity employee that Stanley said he would not accept a cashier’s check because “cashier’s checks don’t work in Europe . . . they won’t cash them in Europe.” As an alternative, FAUST suggested that someone in the company wire the entire payment from their “personal account.” After the employee replied that nobody at

the company was willing to do that, FAUST reminded the employee that Stanley wanted some kind of “resolution” that day.

21. Later that same day, FAUST again called Generational Equity from an unknown telephone number. During the call, which was consensually recorded, FAUST told the same Generational Equity employee that Stanley “might be willing to take . . . payments” from the money-transfer business MoneyGram. Towards the end of the call, FAUST stated that Stanley had told her that the payment amounts would have to be under \$7,500.00 USD to avoid U.S. currency reporting requirements.

22. On January 28, 2014, FAUST, using the e-mail address reputationlynn@gmail.com, sent an e-mail to Generational Equity stating, “Bill wanted me to remind you of the invoiced amount of \$28,556.21 plus my \$1,000.00 legal fee. I am not getting paid a whole lot to do this deal so I am hoping we can get it done sooner than later.”

23. That same day, FAUST called Generational Equity from telephone number [REDACTED]-3559 and left a voice mail. In the voice mail, which was consensually-recorded, FAUST stated, “Bill said to tell you that if he doesn’t hear from somebody very soon, he’s tacking on more collection fees.”

24. Between on or about January 30, 2014, and on or about February 10, 2014, Generational Equity sent four equal payments of \$7,389.05 USD, which totaled \$29,556.20 USD, to Stanley in Romania via MoneyGram. In a prior e-mail, Stanley had instructed Generational Equity to send the money to him in Brasov, Romania, in the

name of "William L. Stanley." The FBI was able to confirm through a MoneyGram representative that all four payments were picked up at the same MoneyGram authorized-agent location in Brasov and that all MoneyGram authorized-agent locations were required to request valid identification from an intended recipient before dispensing money to that recipient.

25. On February 27, 2014, Stanley was arrested on a federal arrest warrant issued out of this investigation for transmitting threats in interstate and foreign commerce upon attempting to enter the United States after arriving at George Bush Intercontinental Airport in Houston, Texas, on a flight from Europe. Following his arrest and after being advised of his constitutional rights and waiving those rights, Stanley was interviewed and provided a statement to Affiant. Specifically, Stanley admitted, among other things, that (1) he had sent threatening e-mails to Generational Equity in order to collect the debt he believed was owed to him by The March Group, (2) that he had posted a negative blog online which identified Generational Equity as a "scam," (3) that his sister, LYNN FAUST, did most of the negotiating with Generational Equity for collection of the debt and used the alias "Lynn Michaels" during those interactions, and (4) that he had received four payments from Generational Equity totaling approximately \$28,000 which he obtained via the money-transfer business, MoneyGram.

26. On or about December 12, 2014, a Plea Agreement and Factual Resume signed by Stanley, his attorney, and the government were filed in this case. A rearraignment date has not been set yet.

FAUST PROCEDURAL STATUS

27. The FBI determined that during the offense FAUST had been living in Greece, but after Stanley was arrested, FAUST moved to Sweden. On or about May 19, 2014, at the request of the FBI, Swedish authorities arrested FAUST pursuant to an issued INTERPOL Red Notice as well as an official Request for Provisional Arrest from the U.S. Department of Justice. The United States submitted its extradition request. In October 2014, FAUST withdrew her opposition to the extradition request, and the United States Marshal transported FAUST from Sweden to the Northern District of Texas. On or about October 16, 2014, Faust initially appeared in the Northern District of Texas with Stanley's attorney Mr. Teakell. Several months passed while Mr. Teakell attempted to represent both Stanley and FAUST. Finally on January 23, 2015, the United States Magistrate Judge Ramirez conducted a Fed. R. Crim. P. 44(c)(1) hearing and appointed FAUST separate counsel.

28. Immediately following FAUST's arrest, Swedish authorities searched the apartment in which FAUST was arrested for items associated with the charged offenses after receiving the requisite authorization from the Swedish prosecutor to do so.⁶ The official Request for Provisional Arrest sent to the Swedish government from the U.S. Department of Justice also requested that all articles relevant to the charged offenses be seized for subsequent surrender to U.S. authorities. During the search following

⁶ Affiant spoke with the FBI's Assistant Legal Attaché in Stockholm, Sweden, who indicated that, under Swedish law, Swedish prosecutors can authorize the search of a dwelling following an arrest and the subsequent seizure of pertinent evidence much like judges in the U.S. do.

FAUST's arrest, Swedish authorities seized several items relevant to the charged offenses, including the Target Devices. On or about June 19, 2014, Swedish authorities turned over the seized items, including the Target Devices, to the FBI's Assistant Legal Attaché in Stockholm, Sweden, who in turn forwarded them to the Dallas office of the FBI. Accordingly, this warrant is being sought to ensure that an examination of the Target Devices will comply with the Fourth Amendment and other applicable laws.

29. The Target Devices are currently in storage at the FBI, One Justice Way, Dallas, Texas, 75220. In my training and experience, I know that the Target Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Target Devices first came into the possession of the FBI.

TECHNICAL TERMS

30. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Laptop computer: A laptop computer, or notebook, is a mobile computer that is typically smaller than a desktop computer. Laptop computers function as wireless communication devices and can be used to access the Internet through Ethernet connections, cellular networks, "wi-fi" networks, or otherwise. Laptop computers typically contain various programs, which perform different functions and save data associated with those functions. The programs can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- b. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone

number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory/thumbdrives, CD-ROMs, and other magnetic or optical media.
- d. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- e. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- f. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock.

Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- g. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.
- h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

31. Based on my training, experience, and research, I know that many electronic items, such as the Target Devices, can have multiple capabilities and therefore can be used for multiple purposes. For instance, from consulting the manufacturer's

advertisements and product technical specifications available online at <http://www.htc.com/us/smartphones/htc-wp-8x/>, I know one of the Target Devices—the HTC cellular telephone with serial number HT2BMW600489--has capabilities that allow it to serve a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

32. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

33. There is probable cause to believe that things that were once stored on the Target Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

34. *Forensic evidence.* As further described in Attachment A, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the charged offenses described above, but also forensic evidence that establishes how the Devices were used, the purposes of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Target Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically-stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to further an alleged offense, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that electronic devices used to commit a crime of this type may contain: data that is evidence of how the electronic devices were used; data that was sent or received; and other records that indicate the nature of the offense.

35. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether they are evidence described by the warrant.

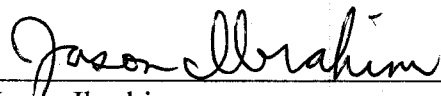
36. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant

does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

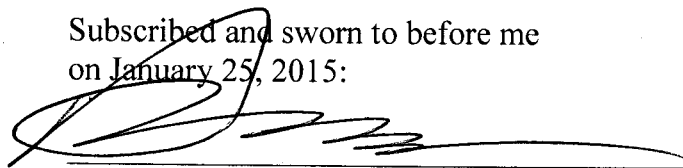
37. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Target Devices to seek the items described in Attachment A.

Respectfully submitted,



Jason Ibrahim
Special Agent
FBI

Subscribed and sworn to before me
on January 25, 2015:



DAVID L. HORAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

1. All records and information on the following three electronic devices
(Target Devices):

- a Hewlett Packard Pavilion DV7-6C95DX laptop computer with serial number 2CE21616QT,
- an HTC cellular telephone with serial number HT2BMW600489, and
- an ATIVA 4GB thumb drive containing the alphanumeric sequences AJDON4GB-000-1002P and 33249-4GBCA-0211.

that relate to Aiding and Abetting and Transmitting Threats in Interstate and Foreign Commerce, in violation of 18 U.S.C. §§ 875(d) and 2, and Aiding and Abetting and Hobbs Act – Extortion, in violation of 18 U.S.C. §§ 1951(a) and 2, and involve LYNN STANLEY FAUST, aka “Lynn Michaels,” and William Laurence Stanley since November 4, 2009, including:

- a. Records and information relating to efforts to threaten, extort, and/or communicate with the victim-business Generational Equity, The March Group, and other victims of similar-type offenses;
- b. Records and information relating to invoices, contracts, and purported debts of Generational Equity, The March Group, and other victims of similar-type offenses;
- c. Records and information relating to the e-mail accounts
reputationrewards@gmail.com, reputationlynn@gmail.com,
reputationmatrix@gmail.com, completereputation@gmail.com,

postingshowcase@gmail.com, and lynn.faust@yahoo.com, and any other e-mail accounts used in the charged offenses or similar-type offenses;

- d. Records and information relating to bank/financial accounts, bank/financial transactions, checks, credit/debit cards, wire transfers, and other records pertaining to financial activity conducted in furtherance of the charged offenses or similar-type offenses;
- e. Records and information, including names, addresses, phone numbers, or any other identifying information, regarding individuals involved in the charged offenses or similar-type offenses as well as victims of the charged offenses or similar-type offenses;
- f. Records and information, including GPS data, relating to the identities, locations, and travel of the subjects; and
- g. Records and information relating to communications with William Stanley and other individuals, both known and unknown, who are involved in the offenses.

2. Evidence of user attribution showing who used or owned the Target Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

3. Records evidencing the use of the Target Devices to communicate with website servers associated with the charged offenses (e.g., Google Mail servers, Google Voice servers, FreshBooks servers) including:

- a. records of Internet Protocol addresses used; and
- b. records of Internet activity, including application logs, firewall logs, system logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.